Claims remaining in the application are as follows:

1. (Currently amended): A Personal Identification Number (PIN) verification apparatus comprising:

> a plurality of cipher blocks linked in a Cipher Block Chain (CBC) and keyed with a secret PIN Verification Key (PVK);
>
> a first input block coupled to a first cipher block in the CBC chain that receives a ~~text~~ first plaintext block derived from a secret Personal Identification Number (PIN); and
>
> a second input block coupled to a second cipher block in the CBC chain that receives a ~~text~~ second plaintext block derived from a non-secret entity-identifier independent of the PIN and receives ciphertext from a cipher block in the CBC chain.

2. (Currently amended): The apparatus according to Claim 1 further comprising:

> a logical operator that exclusive-ORs the first plaintext block derived from the secret PIN with an initialization vector to produce an initialized block;
>
> a first encryptor that encrypts the initialized block using triple Data Encryption Standard (3-DES) encryption to produce a first ciphertext block;
>
> a logical operator that exclusive-ORs the second plaintext block derived from the non-secret entity-identifier independent of the PIN with the first ciphertext block to produce a chained block; and
>
> a second encryptor that encrypts the chained block using triple Data Encryption Standard (3-DES) encryption to produce a second ciphertext block.

3. (Previously presented):   The apparatus according to Claim 2 wherein:

   the PIN verification apparatus operates in a reversible mode that recovers the
       secret PIN from the second ciphertext block.

4. (Original):   The apparatus according to Claim 2 further comprising:

   a logical operator that exclusive-ORs the first ciphertext block with the second
       ciphertext block to produce a third ciphertext block.

5. (Original):   The apparatus according to Claim 4 wherein:

   the PIN verification apparatus operates in an irreversible mode that obstructs
       recovery of the secret PIN.

6. (Previously presented):   The apparatus according to Claim 5 further comprising:

   an escrow storage coupled to the second encryptor that stores the second
       ciphertext block.

7. (Original):   The apparatus according to Claim 1 further comprising:

   the plurality of cipher blocks that encrypt data according to a triple Data
       Encryption Standard (3-DES).

8. (Previously presented): The apparatus according to Claim 1 further comprising:

   a format converter coupled to a cipher block in the CBC chain that converts
       hexadecimal digit ciphertext to a decimal result by receiving in
       sequence the hexadecimal digit ciphertext, selecting a predetermined
       number of numeric digits, and generating output digits as a PIN
       Verification Value (PVV).

9. (Original):   The apparatus according to Claim 1 further comprising:
the plurality of cipher blocks that encrypt data according to a definition
        selected from among a group consisting of triple Data Encryption
        Standard (3-DES) and Advanced Encryption Standard (AES) definition.

10. (Currently amended): The apparatus according to Claim 1 further
comprising:
        a first formatter that constructs a first incoming plaintext block from a
                concatenation of a length digit, x hexadecimal digits of the secret
                Personal Identification Number (PIN) with 16-(x+1) rightmost
                hexadecimal digits of the non-secret entity-identifier; and
        a second formatter that constructs a second incoming plaintext block
                independent of the PIN from a concatenation of y hexadecimal digits of
                the non-secret entity-identifier with a pad character that is repeated 16-
                y times.

11. (Currently amended): A method for Personal Identification Number (PIN)
verification comprising:
        linking a plurality of cipher blocks in a Cipher Block Chain (CBC);
        applying ~~an incoming~~ a first incoming plaintext block derived from a secret
                Personal Identification Number (PIN) to one of the plurality of cipher
                blocks;
        applying ~~an incoming~~ a second incoming plaintext block derived from a non-
                secret entity-identifier independent of the PIN and ciphertext from a
                cipher block in the CBC chain to a second of the plurality of cipher
                blocks;
        keying the plurality of cipher blocks with a secret PIN Verification Key (PVK);
                and
        executing the plurality of cipher blocks ~~resulting in generation of~~ wherein
                ciphertext is generated.

12. (Currently amended): The method according to Claim 11 further comprising:

a plurality of cipher blocks that encrypt encrypting data according to a triple Data Encryption Standard (3-DES) using a plurality of cipher blocks.

13. (Currently amended): The method according to Claim 11 wherein the PIN verification method is capable of further comprises:

operating in a reversible mode that enables recovery of the secret PIN, the method comprising: PIN;

exclusive-ORing the first incoming plaintext block derived from the secret PIN with an initialization vector to produce an initialized block;

encrypting the initialized block using triple Data Encryption Standard (3-DES) encryption to produce a first ciphertext block;

exclusive-ORing the second incoming plaintext block derived from the non-secret entity-identifier independent of the PIN with the first ciphertext block to produce a chained block;

encrypting the chained block using triple Data Encryption Standard (3-DES) encryption to produce a second ciphertext block; and

supplying the second ciphertext block for PIN verification.

14. (Currently amended): The method according to Claim 11 wherein the PIN verification method is capable of further comprises:

operating in an irreversible mode that obstructs recovery of the secret PIN, the method comprising: PIN;

exclusive-ORing the first incoming plaintext block derived from the secret PIN with an initialization vector to produce an initialized block;

encrypting the initialized block using triple Data Encryption Standard (3-DES) encryption to produce a first ciphertext block;

exclusive-ORing the second incoming plaintext block derived from the non-secret entity-identifier independent of the PIN with the first ciphertext block to produce a chained block;

encrypting the chained block using triple Data Encryption Standard (3-DES)

encryption to produce a second ciphertext block;

exclusive-ORing the first ciphertext block with the second ciphertext block to

produce a third ciphertext block; and

supplying the second ciphertext block for PIN verification.

15. (Original):   The method according to Claim 14 further comprising:

storing the second ciphertext block in at least one escrow to facilitate recovery

of the secret PIN.

16. (Previously presented):   The method according to Claim 11 further

comprising:

converting hexadecimal digit ciphertext generated by a final ciphertext block in

the Cipher Block Chain (CBC) to a decimal result by receiving in

sequence the hexadecimal digit ciphertext, selecting a predetermined

number of numeric digits, and generating output digits as a PIN

Verification Value (PVV); and

using the PVV for PIN verification.

17. (Original):   The method according to Claim 11 further comprising:

supplying hexadecimal digit ciphertext generated by a final ciphertext block in

the Cipher Block Chain (CBC) as a PIN Verification Value (PVV).

18. (Original):   The method according to Claim 11 further comprising:

a plurality of cipher blocks that encrypt data according to a definition selected

from among a group consisting of triple Data Encryption Standard (3-

DES) and Advanced Encryption Standard (AES) definition.

19. (Currently amended): The method according to Claim 11 further

comprising:

constructing a first the first incoming plaintext block from a concatenation of a

length digit, x hexadecimal digits of the secret Personal Identification

KOESTNER BERTANI LLP

2192 MARTIN ST.
SUITE 150
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

Number (PIN) with 16-(x+1) rightmost hexadecimal digits of the non-secret entity-identifier; and

constructing ~~a second~~ the second incoming plaintext block from a concatenation of y hexadecimal digits of the non-secret entity-identifier with a pad character that is repeated 16-y times wherein the second incoming plaintext block is independent of the PIN .

20. (Currently amended): A data security apparatus comprising:

an enrollment terminal configured to accept ~~capable of accepting a magnetic stripe card storing a non-secret entity-identifier and~~ an entity-selected secret Personal Identification Number (PIN) and a magnetic stripe card storing a non-secret entity-identifier independent of the PIN;

a processor coupled to the enrollment terminal that receives the entity-identifier and the PIN; and

a memory coupled to the processor and having a computable readable program code embodied therein capable of causing the processor to enroll a PIN comprising linking a plurality of cipher blocks in a Cipher Block Chain (CBC), applying an incoming first plaintext block derived from the secret Personal Identification Number (PIN) to one of the plurality of cipher blocks, applying an incoming second plaintext block derived from the non-secret entity-identifier that is independent of the PIN and ciphertext from a cipher block in the CBC chain, keying the plurality of cipher blocks with a secret PIN Verification Key (PVK), and executing the cipher blocks resulting in generation of ciphertext PIN Verification Value (PVV) for usage in performing a subsequent PIN verification function.

21. (Currently amended): The apparatus according to Claim 20 wherein the PIN verification function is ~~capable of operating~~ configured to operate in a reversible mode that enables recovery of the secret PIN and the memory further comprises:

a computable readable program code capable of causing the processor to exclusive-OR the first plaintext block derived from the secret PIN with an initialization vector to produce an initialized block;

a computable readable program code capable of causing the controller to encrypt the initialized block using triple Data Encryption Standard (3-DES) encryption to produce a first ciphertext block;

a computable readable program code capable of causing the controller to exclusive-OR the second plaintext block derived from the non-secret entity-identifier that is independent of the PIN with the first ciphertext block to produce a chained block;

a computable readable program code capable of causing the controller to encrypt the chained block using triple Data Encryption Standard (3-DES) encryption to produce a second ciphertext block; and

a computable readable program code capable of causing the controller to supply the second ciphertext block for PIN verification.

22. (Currently amended): The apparatus according to Claim 20 wherein the PIN verification function is ~~capable of operating~~ configured to operate in an irreversible mode that obstructs recovery of the secret PIN and the memory further comprises:

a computable readable program code capable of causing the processor to exclusive-OR the first plaintext block derived from the secret PIN with an initialization vector to produce an initialized block;

a computable readable program code capable of causing the controller to encrypt the initialized block using triple Data Encryption Standard (3-DES) encryption to produce a first ciphertext block;

a computable readable program code capable of causing the controller to exclusive-OR the second plaintext block derived from the non-secret entity-identifier that is independent of the PIN with the first ciphertext block to produce a chained block;

a computable readable program code capable of causing the controller to encrypt the chained block using triple Data Encryption Standard (3-DES) encryption to produce a second ciphertext block;

a computable readable program code capable of causing the controller to exclusive-OR the first ciphertext block with the second ciphertext block to produce a third ciphertext block; and

a computable readable program code capable of causing the controller to supply the second ciphertext block for PIN verification.

23. (Original):   The apparatus according to Claim 22 further comprising:

an escrow storage communicatively coupled to the transaction system and comprising at least one escrow storage element; and

the memory further comprises a computable readable program code capable of causing the processor to store the second ciphertext block in the escrow storage in at least one secret escrow share to facilitate recovery of the secret PIN.

24. (Previously presented):   The apparatus according to Claim 20 wherein the memory further comprises:

a computable readable program code capable of causing the processor to convert hexadecimal digit ciphertext generated by a final ciphertext block in the Cipher Block Chain (CBC) to a decimal result by receiving in sequence the hexadecimal digit ciphertext, selecting a predetermined number of numeric digits, and generating output digits as a PIN Verification Value (PVV); and

a computable readable program code capable of causing the processor to write the PVV to a magnetic stripe card or a smart card.

25. (Original):   The apparatus according to Claim 20 wherein the memory further comprises:

a computable readable program code capable of causing the processor to store hexadecimal digit ciphertext generated by a final ciphertext block

in the Cipher Block Chain (CBC) as a PIN Verification Value (PVV) in a storage element.

26. (Original):   The apparatus according to Claim 20 wherein:

the plurality of cipher blocks encrypt data according to a definition selected from among a group consisting of triple Data Encryption Standard (3-DES) and Advanced Encryption Standard (AES) definition.

27. (Currently amended): The apparatus according to Claim 20 wherein the memory further comprises:

a computable readable program code capable of causing the processor to construct ~~a first~~ the first incoming plaintext block from a concatenation of a length digit and x hexadecimal digits of the secret Personal Identification Number (PIN) with 16-(x+1) rightmost hexadecimal digits of the non-secret entity-identifier; and

a computable readable program code capable of causing the processor to construct ~~a second~~ the second incoming plaintext block from a concatenation of y hexadecimal digits of the non-secret entity-identifier with a pad character that is repeated 16-y times <u>wherein the second incoming plaintext block is independent of the PIN</u>.

28. (Currently amended): A data security apparatus comprising:

a PIN Verification Value (PVV) database ~~capable of storing~~ <u>configured to store</u> a plurality of PIN Verification Values (PVVs) for enrolled magnetic stripe cards;

an escrow ~~capable of storing~~ <u>configured to store</u> a plurality of escrow values associated with at least some of the enrolled magnetic stripe cards; and

a processor coupled to the PVV database and the escrow that receives an entity-identifier, a PIN Verification Value (PVV) associated to the entity-identifier, and at least one escrow value associated to the entity-identifier; and

KOESTNER BERTANI LLP

2192 MARTIN ST.
SUITE 150
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

a memory coupled to the processor and having a computable readable

program code embodied therein capable of causing the processor to

recover a PIN comprising linking a plurality of cipher blocks in a Cipher

Block Chain (CBC), applying an incoming first plaintext block derived

from the PIN Verification Value (PVV) to one of the plurality of cipher

blocks, applying an incoming second plaintext block derived from the

non-secret entity-identifier that is independent of the PIN and ciphertext

from a cipher block in the CBC chain, keying the plurality of cipher

blocks with a secret PIN Verification Key (PVK), executing the cipher

blocks to produce a ciphertext value, and combining the ciphertext

value with the at least one escrow value resulting in recovery of the PIN

verification function.

29. (Currently amended): A data security apparatus comprising:

a transaction terminal adapted to accept ~~capable of accepting a magnetic~~

~~stripe card storing a non-secret entity-identifier and~~ an entity-entered

secret Personal Identification Number (PIN') and a magnetic stripe card

storing a non-secret entity-identifier independent of the PIN;

a PIN Verification Value (PVV) database;

a processor communicatively coupled to the transaction terminal that receives

the entity-identifier, the PIN', and coupled to the PVV database ~~and~~

~~capable of~~ for retrieving a PIN Verification Value (PVV) associated with

the entity-identifier; and

a memory coupled to the processor and having a computable readable

program code embodied therein capable of causing the processor to

verify the PIN' comprising linking a plurality of cipher blocks in a Cipher

Block Chain (CBC), applying an incoming first plaintext block derived

from the secret entered Personal Identification Number (PIN') to one of

the plurality of cipher blocks, applying an incoming second plaintext

block derived from the non-secret entity-identifier independent of the

PIN' and ciphertext from a cipher block in the CBC chain, keying the

plurality of cipher blocks with a secret PIN Verification Key (PVK), executing the cipher blocks resulting in generation of ciphertext transaction PIN Verification Value (PVV'); comparing the generated PVV' and the retrieved PVV; and determining PIN verification based on the comparison.

30. (Currently amended): A transaction system comprising:

a network;

a plurality of servers and/or hosts coupled to the network;

a plurality of terminals coupled to the servers via the network;

a plurality of magnetic stripe cards enrolled in the transaction system and

> ~~capable of~~ configured for insertion into the on-line terminals and
> performing transactions via the servers; and

a plurality of processors distributed among the servers, hosts, and/or the

> terminals, at least one of the processors being capable of executing
> PIN verification using a magnetic stripe card and having a computable
> readable program code embodied therein capable of causing the
> processor to link a plurality of cipher blocks in a Cipher Block Chain
> (CBC), apply an incoming first plaintext block derived from a secret
> Personal Identification Number (PIN) to one of the plurality of cipher
> blocks, apply an incoming second plaintext block derived from a non-
> secret entity-identifier independent of the PIN and ciphertext from a
> cipher block in the CBC chain, key the plurality of cipher blocks with a
> secret PIN Verification Key (PVK), and execute the cipher blocks
> resulting in generation of ciphertext.

31. (Currently amended): A data security apparatus comprising:

means for enrolling a transaction card in a data system; and

means for generating a Personal Identification Number (PIN) Verification

> Value (PVV) for usage in Personal Identification Number (PIN)
> verification further comprising:

means for linking a plurality of cipher blocks in a Cipher Block Chain (CBC);

means for applying an incoming <u>first</u> plaintext block derived from a secret Personal Identification Number (PIN) to one of the plurality of cipher blocks;

means for applying an incoming <u>second</u> plaintext block derived from a non-secret entity-identifier <u>independent of the PIN</u> to another of the plurality of cipher blocks;

means for keying the plurality of cipher blocks with a secret PIN Verification Key (PVK); and

means for generating a PIN Verification Value (PVV) via operation of a plurality of cipher blocks in the Cipher Block Chain; and

means for writing the PVV to a transaction card for subsequent PIN verification.